




# **POLÍTICA USO DE TECNOLOGÍAS DE INFORMACIÓN**

**CÓDIGO: AAA-POL-015**


**REVISIÓN: 01**

**2022**

 <p><b>ABONOS AGRO</b></p>	<h2>Política Uso de Tecnologías de Información</h2>	Código	AAA-POL-015
		Revisión	1
		Fecha	
		Realizado por	Gestión de Procesos
		Aprobado por	

## ÍNDICE

<b>1. OBJETIVO</b> .....	<b>3</b>
<b>2. ALCANCE</b> .....	<b>3</b>
<b>3. DEFINICIONES Y ABREVIATURAS</b> .....	<b>3</b>
3.1. Comunicaciones electrónicas: .....	3
3.2. Material no permitido.....	3
3.3. Red de datos: .....	4
3.4. Redes:.....	4
3.5. Sistemas de Información.....	4
3.6. Usuario(s):.....	4
3.7. Negligencia.....	4
3.8. Imprudencia .....	4
3.9. Impericia .....	4
<b>4. BASE LEGAL</b> .....	<b>4</b>
<input type="checkbox"/> <i>Artículo 36 Deudas del trabajador</i> .....	4
<input type="checkbox"/> <i>Artículo 71 Obligaciones de los trabajadores</i> .....	4
<input type="checkbox"/> <i>Artículo 81 Causas de despido</i> .....	4
<input type="checkbox"/> <i>Artículo 172 Salario. Embargo. Procedimiento</i> .....	4
<input type="checkbox"/> <i>Artículo 173 Anticipo del patrono al trabajador</i> .....	4
<b>5. POLÍTICAS</b> .....	<b>5</b>
5.1. Generalidades .....	5
5.2. Uso permitido de la Red de Datos .....	6
5.3. Equipos de cómputo y periféricos .....	6
5.4. Dispositivos de impresión .....	8
5.5. Dispositivos de colaboración .....	8
5.6. Acceso a la Red Empresarial y a sus servicios.....	8
5.7. Uso indebido y prohibiciones en el uso de las redes, las comunicaciones electrónicas y sistemas de información .....	10
5.8. Privacidad.....	12
5.9. Instalación y Uso de Software .....	14
5.10. Correo electrónico y demás herramientas colaborativas disponibles ...	14
5.11. Páginas Web y Sistema de contenido en Redes Sociales.....	15
5.12. Incumplimiento de las políticas de uso responsable de los sistemas de información y recursos informáticos de la organización .....	15
<b>6. RESPONSABLES</b> .....	<b>16</b>
<b>7. ANEXOS</b> .....	<b>18</b>
7.1. Anexo N°1. Contrato de condiciones de entrega y uso de herramientas de Tecnologías de Información propiedad de Aceros Abonos Agro .....	18
7.2 Anexo N°2. Proceso de Investigación .....	22
<b>8. CONTROL DE CAMBIOS</b> .....	<b>22</b>

	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

## 1. OBJETIVO

El propósito de este documento es definir la Política Organizacional con respecto al uso y prohibiciones de los sistemas de información en Aceros Abonos Agro.

Todo colaborador y tercero autorizado por la empresa, deberá seguir las normas, políticas y buenas prácticas establecidas en la presente política.

## 2. ALCANCE


Esta política se aplicará a todos los colaboradores, proveedores, contratistas, consultores, aprendices y a cualquier otra persona que tenga acceso a los sistemas de información de la Organización.

También se aplica esta política a todos los equipos y sistemas informáticos: servidores, computadores personales, estaciones de trabajo, elementos de infraestructura tecnológica, dispositivos móviles, portátiles, asistentes digitales personales, bases de datos, sistemas de información que apoyan los procesos de producción o administrativos que se encuentren bajo responsabilidad operacional de Aceros Abonos Agro, así como también a aquellos dispositivos de uso personal que ingresen a la misma.

## 3. DEFINICIONES Y ABREVIATURAS

Para los propósitos de esta política se aplicarán las siguientes definiciones:

- 3.1. **Comunicaciones electrónicas:** Incluye todo uso de los sistemas de información para comunicar, publicar material y contenido por medio de servicios como correo electrónico, chats, foros de discusión, paginas HTML o - herramientas similares.
- 3.2. **Material no permitido:** Incluye la transmisión, distribución o almacenamiento de todo material que viole cualquier ley aplicable. Se incluye sin limitación, correos electrónicos de tipo cadena, material protegido por derechos de reproducción, marca comercial, secreto comercial, u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio, ilegal bajo las leyes nacionales, racismo, violencia y demás contenidos que contravengan los principios y valores socialmente aceptados.


	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

- 3.3. Red de datos:** Es el conjunto de recursos de conectividad computacionales que permite la comunicación de datos e información a través de toda la Organización incluyendo el correo interno, externo e Internet.
- 3.4. Redes:** Incluye cualquier sistema de cableado o inalámbrico; equipos físicos como enrutadores, switches, además de sistemas electrónicos como redes de video, datos, voz y dispositivos de almacenamiento.
- 3.5. Sistemas de Información:** Incluye cualquier sistema o aplicación de software que sea administrado por la Organización y de los cuales ella es responsable, además, aplicaciones de servidores y escritorio, sistemas operativos y aplicaciones de Internet.
- 3.6. Usuario(s):** Incluye toda persona no necesariamente vinculada con la empresa, a quien ésta proporcione los medios y niveles de automatización y acceso necesarios para hacer uso de los servicios o sistemas de información de ésta.
- 3.7. Negligencia:** Falta de cuidado, aplicación y diligencia de una persona en lo que hace, en especial en el cumplimiento de una obligación.
- 3.8. Imprudencia:** Es la falta de precaución que implica omitir la diligencia requerida. Se trata de un olvido de la previsión aconsejable para realizar algún hecho que la prudencia popular recomendaría.
- 3.9. Impericia:** falta total o parcial de conocimientos técnicos, experiencia o habilidad para el desempeño profesional.

#### 4. BASE LEGAL

Esta política tiene su base legal según el **Código de Trabajo de Costa Rica** actualizado con la Reforma Procesal Laboral estipulada según el Ministerio de Trabajo y Seguridad Social. Los artículos que se nombran en el desarrollo de la política se presentan a continuación:

- *Artículo 36 Deudas del trabajador*
- *Artículo 71 Obligaciones de los trabajadores*
- *Artículo 81 Causas de despido*
- *Artículo 172 Salario. Embargo. Procedimiento*
- *Artículo 173 Anticipo del patrono al trabajador*


	<b>Política Uso de Tecnologías de Información</b>	Código	AAA-POL-015
		Revisión	1
		Fecha	
		Realizado por	Gestión de Procesos
		Aprobado por	

## 5. POLÍTICAS

### 5.1. Generalidades

Aceros Abonos Agro provee el acceso a todo el personal a fuentes de información nacional e internacional y promueve un ambiente digital que fomente la difusión del conocimiento, el proceso de creación y el trabajo colaborativo, en el marco del Propósito Superior de la Organización.

- ✓ Los usuarios deben hacer uso responsable y ético. Cada usuario es responsable por la integridad de estos recursos y tiene el deber de respetar los derechos de los otros usuarios, la integridad de las instalaciones físicas y sus métodos de control, además de respetar toda licencia pertinente y acuerdo contractual que esté relacionado con los sistemas de información de la Organización. Para afirmar tales hechos **se debe proceder con la firma del colaborador** en el **contrato de condiciones de entrega del uso de Herramientas de Tecnologías de Información propiedad de Aceros Abonos Agro (Ver anexo N°1)**
- ✓ Los usuarios tienen la responsabilidad de informar a su jefe inmediato, al responsable de Informática o a quien haga sus veces, de los incidentes relacionados con el uso indebido de los sistemas de información.
- ✓ Aceros Abonos Agro puede restringir o prohibir el uso de sus sistemas de información, en cualquier caso en el que se demuestre alguna violación de estas políticas o de alguna ley de la República.
- ✓ Aceros Abonos Agro no asume responsabilidad alguna por el empleo de “material no permitido” en los contenidos de los correos electrónicos, así como del uso ilegal y mal intencionado del mismo por parte de sus usuarios.
- ✓ Los miembros de la Unidad de Informática están en la obligación de monitorear constantemente los sistemas de información de Aceros Abonos Agro a través de las herramientas informáticas disponibles o a través de auditorías externas para responder a cualquier acción que atente contra la integridad, disponibilidad, seguridad y desempeño correcto de los mismos mediante la negación, restricción de acceso a usuarios o sistemas, aislamiento y desconexión de equipos o servicios.
- ✓ La unidad de informática cuenta con procedimiento para el respaldo y la restauración de los sistemas de información con el objetivo de garantizar la continuidad del negocio frente a una falla y/o desastre.

 <p><b>ABONOS AGRO</b></p>	<h2>Política Uso de Tecnologías de Información</h2>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

- ✓ La unidad de Informática garantizará que las versiones de los sistemas operativos usados en la empresa estén actualizados a las últimas versiones con el fin de evitar que alguna vulnerabilidad detectada, pueda ser aprovechada por un virus o atacante.
- ✓ La Dirección de informática es la única dependencia autorizada para avalar la contratación de cualquier servicio tecnológico requerido, incluyendo, pero sin limitar, internet, servicios en nube, servidores, equipos de cómputo, Licencias, telefonía, impresión y otros servicios externos.
- ✓ La unidad Informática brindará soporte y mantenimiento sobre recursos y servicios informáticos (Software, hardware, equipos, almacenamiento y hosting, entre otros) que estén dentro del gobierno de soporte y mantenimiento de TI.

Todos los usuarios deberán actuar de acuerdo con estos lineamientos, al reglamento interno de trabajo y/o políticas internas de la compañía, así como a las leyes nacionales o internacionales pertinentes. El incumplimiento de esta política puede resultar en la negación de acceso a los sistemas de información de la Organización o a otras acciones disciplinarias o legales.


Es un compromiso de todos los usuarios de Aceros Abonos Agro, entender y dar cumplimiento a las políticas consignadas en el presente documento, y acatarlas durante el desarrollo de sus actividades.

### 5.2. Uso permitido de la Red de Datos


El uso es permitido primordialmente para asuntos de la Organización. Los sistemas de información de la Organización son únicamente para uso de asuntos relacionados con la misma. El uso personal de los sistemas de información para acceder, descargar, transmitir, distribuir o almacenar “Material no permitido”, está prohibido.

El uso personal de herramientas de oficina, tales como Internet, procesadores de texto y hojas de cálculo entre otros, debe ser limitado y bajo ninguna circunstancia el uso personal de estas herramientas debe influir de manera negativa en el desempeño de las tareas y responsabilidades para con la Organización. En los casos en que se haga uso personal excesivo de estas herramientas, la Organización podrá limitar su acceso.

### 5.3. Equipos de cómputo y periféricos

	<h2>Política Uso de Tecnologías de Información</h2>	Código	AAA-POL-015
		Revisión	1
		Fecha	
		Realizado por	Gestión de Procesos
		Aprobado por	

- ✓ Propender por el cuidado y preservación de las herramientas informáticas y computadores asignados al colaborador.
- ✓ Evitar consumir alimentos y tomar bebidas cerca del equipo asignado. Un incidente de este tipo puede afectar su funcionamiento e incluso dañarlo.
- ✓ Evitar colocar elementos pesados sobre el equipo, en especial portátiles ya que son más frágiles.
- ✓ El colaborador tendrá la responsabilidad de informar y entregar a la Dirección de informática, los recursos y servicios informáticos que no esté utilizando en su trabajo.
- ✓ Los recursos informáticos asignados al colaborador están bajo su responsabilidad. En caso de daño, pérdida o hurto, el colaborador deberá cumplir con lo expuesto en el Contrato (Anexo N°1) asumiendo la responsabilidad, posterior al proceso y resultado de la investigación (Anexo N°2) que realizará la empresa. Talento Humano aplicará el pago mediante anticipo de salario y/o reducción de planilla del respectivo cobro del activo tecnológico y aplicará las oportunas acciones disciplinarias, si es encontrada la negligencia por parte del colaborador.
- ✓ En caso de requerir retirar de la empresa cualquier recurso informático no asignado al cargo, es deber del colaborador pedir las autorizaciones necesarias.
- ✓ Cualquier colaborador que sea responsable de un contrato en el cual se involucren computadores, servidores, licencias y periféricos, sean propios o de propiedad de un tercero, debe solicitar autorización a la jefatura de Informática para el uso y transporte de estos dentro de las instalaciones.
- ✓ El usuario tendrá la obligación de notificar al departamento de Contabilidad y al área de TI de AAA en cumplimiento del **procedimiento “AAA-P-037 Ingreso y Salida de Activos”**, los traslados de los equipos de cómputo (No portátiles) y periféricos.
- ✓ El usuario es responsable de mantener la información resultado de las funciones propias de su rol almacenada en su carpeta de OneDrive o Carpeta de SharePoint, estas son las ubicaciones corporativas a las que la unidad informática les realiza respaldo.

	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

- ✓ Las políticas de retención establecidas por nuestro proveedor de servicios Microsoft, para los elementos eliminados con posibilidad de recuperarlos, son: One Drive: 93 días. SharePoint Online: 93 días. Correo: 14 días.
- ✓ Durante periodos de vacaciones y licencias autorizadas por Talento Humano, no está permitido transportar equipos de cómputo fuera de la organización. Los permisos especiales deberán tramitarse directamente entre Gerentes y/o Jefaturas del área solicitante con previa autorización del Departamento de Talento Humano.

#### **5.4. Dispositivos de impresión**

##### **El colaborador debe:**

- ✓ Velar porque el servicio de impresión sea utilizado para actividades laborales y uso exclusivo de la organización.
- ✓ Propender por el buen uso de las impresoras.
- ✓ Reportar las solicitudes, requerimientos e incidentes correspondientes al servicio de impresión a la mesa de ayuda (Deuna).
- ✓ Realizar un uso adecuado del papel e imprimir siempre y cuando sea estrictamente necesario.
- ✓ No realizar labores de reparación o mantenimiento de las impresoras.


#### **5.5. Dispositivos de colaboración**

- ✓ Cualquier dispositivo de colaboración asignado a un colaborador, como teléfono, cámara, audífonos, diademas, entre otros, quedará bajo su responsabilidad y deberá ser usado para actividades laborales.
- ✓ Ningún colaborador está autorizado para retirar, trasladar o modificar los equipos de las salas de reuniones o capacitación sin previo consentimiento por parte de la Unidad Informática.


#### **5.6. Acceso a la Red Empresarial y a sus servicios**

- ✓ La Organización asignará a cada usuario una identificación y clave de acceso a los servicios informáticos que éste, por la naturaleza de su cargo, requiera.



	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

- ✓ Las identificaciones y claves de acceso a la red empresarial, el Portal Empresarial ALAIA o a cualquier otro Sistema de información son propiedad de la Organización. Estas identificaciones y claves son para uso estrictamente personal e intransferible. La responsabilidad en su manejo recae exclusivamente en el usuario a quien se le asignen. Esta política aplica también para otros factores de autenticación dados por la empresa.
- ✓ El acceso a través de la conexión VPN debe ser solicitado por el Gerente/ Jefatura de cada área para uso de un colaborador o una persona externa con fines netamente laborales. El acceso a este servicio es personal e intransferible, por tanto, el usuario debe abstenerse de compartirse con personas no autorizadas. El colaborador es responsable de que el computador utilizado por el tercero para la conexión remota posea las actualizaciones más recientes de sistema operativo y antivirus.
- ✓ El acceso no autorizado a los sistemas de información de la Organización está prohibido. Ningún colaborador debe usar la identificación, identidad o contraseña de otro usuario, y de la misma manera ningún usuario debe dar a conocer su contraseña o identificación a otro, excepto en casos que faciliten la reparación o el mantenimiento de algún servicio o equipo y en este caso debe dar a conocer estos datos única y exclusivamente a miembros de la Unidad de Informática de la Organización. En el caso en que este evento se dé, el usuario está en la obligación de cambiar su(s) clave(s) dadas a conocer a Informática inmediatamente se restablezca el servicio o equipo.
- ✓ El usuario no deberá, sin permiso escrito de la Organización, hacer modificaciones a la Red de datos, la Intranet o sus recursos. No se permitirá ningún intento de vulnerar o de atentar contra los sistemas de protección o de seguridad de la red. Ante cualquier acción de este tipo, la Organización procederá a ejecutar cualquier acción de carácter administrativo, laboral, penal y/o civil que corresponda.
- ✓ En la red empresarial no está permitida la operación de software para la descarga y distribución de archivos de música, videos y similares. Cualquier aplicación de este tipo que requiera ser utilizada, deberá ser previamente autorizada por la Unidad de Informática con el visto bueno del Gerente y/o Jefatura de área respectiva. Adicionalmente, no está permitido almacenar archivos de música, videos y similares de índole personal en el disco duro del equipo asignado al usuario o en su espacio asignado en la nube corporativa.


	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

- ✓ El acceso a internet en la Organización debe hacerse desde una estación o dispositivo debidamente registrado y/o autorizado por la Unidad de Informática. Dicho de otra forma, el computador debe estar registrado dentro del DNS (Domain Name Server) primario de la Organización y estar localizado con una dirección IP legítima (validada por la Unidad de Informática). Adicionalmente, se asignan perfiles de navegación al colaborador de acuerdo con el cargo.


### **5.7. Uso indebido y prohibiciones en el uso de las redes, las comunicaciones electrónicas y sistemas de información**

A continuación, se enuncian las acciones prohibidas en el uso de las redes, comunicaciones electrónicas y sistemas de información. Lo cual es meramente enunciativa más no taxativa, de tal manera que cualquier actividad que, aunque no se encuentre en esta lista, cause perjuicio a los sistemas de información, a las personas o a la empresa, se considerará un uso indebido y estará sujeta a las acciones disciplinarias que la empresa estime conveniente:

- ✓ Manipular cualquier dispositivo para ingresar a la red cableada o inalámbrica de la Organización sin la previa autorización de la Unidad de Informática.
- ✓ Modificar, desconectar, reubicar o sustraer del lugar donde han sido instalados o configurados, equipos de cómputo, sistemas de información o periféricos sin la debida autorización de la unidad Informática.
- ✓ Interferir sin autorización el acceso de otros usuarios a los recursos de los sistemas de información de la Organización.
- ✓ Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- ✓ Utilizar los sistemas de información para propósitos ilegales o no autorizados.
- ✓ Enviar cualquier comunicación electrónica fraudulenta.
- ✓ Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente sin la autorización escrita del propietario del software.

	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	


- ✓ Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.
- ✓ Usar las comunicaciones electrónicas para acosar o amenazar a los usuarios de la Organización o externos.
- ✓ Usar las comunicaciones electrónicas para revelar información privada sin la autorización explícita de la empresa.
- ✓ Usar el correo electrónico corporativo para campañas masivas hacia terceros, ya que pueden comprometer la calificación de nuestro dominio como emisor de SPAM.
- ✓ Hacer Uso de recursos web y servicios de almacenamiento compartidos, que no sean autorizados por la Unidad informática.
- ✓ Leer la información o archivos de otros usuarios sin su autorización.
- ✓ Realizar actividades dentro de una sesión que le pertenece a otro usuario al encontrar la sesión abierta.
- ✓ Alterar o falsificar de manera fraudulenta los registros de la Organización, incluyendo registros computarizados, permisos, documentos de identificación, u otros documentos o propiedades.
- ✓ Usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
- ✓ Usar las comunicaciones electrónicas para apropiarse de los documentos de otros usuarios.
- ✓ Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil, destructiva o intente vulnerar la seguridad de la red informática y sus sistemas de información.
- ✓ Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Organización.
- ✓ Transportar o almacenar material con derechos de propiedad intelectual o material no permitido usando los equipos o las redes de la Organización.

	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

- ✓ Utilizar cualquier sistema de información de la Organización para acceder, descargar, imprimir, almacenar, reenviar, transmitir o distribuir material no permitido o correos electrónicos de tipo “cadenas”.
- ✓ Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.
- ✓ Usar, instalar software de espionaje, monitoreo de tráfico o programas maliciosos en la red de la empresa.
- ✓ Instalar, Introducir cualquier tipo de programa en la red o equipos sin la debida autorización de la Unidad informática.
- ✓ Efectuar violaciones a la seguridad o interrupciones de la comunicación de la red. Las violaciones de seguridad incluyen la instalación o utilización de “sniffer”, “flooders”, “Packet Spoofing”, negación del servicio (DOS), manipulación de ruteo, etc.
- ✓ Monitorear o escanear puertos de servidores o switches.
- ✓ Evitar o interceptar la autenticación de cualquier usuario por cualquier método.
- ✓ Usar cualquier método (exploits, scripts, comandos) para acceder a recursos a los que no se tiene acceso o a áreas protegidas.
- ✓ Sustraer cualquier tipo información sensible o confidencial del negocio con fines diferentes a los laborales por medio de dispositivos de almacenamiento extraíble o correo electrónico.


## **5.8. Privacidad**

- ✓ La privacidad de los usuarios no está garantizada. Cuando los sistemas de información de la Organización funcionan correctamente, un usuario puede considerar que sus datos generados son información privada, a menos que él mismo realice alguna acción para revelarlos a otros. Los usuarios deben ser conscientes que ningún sistema de información es completamente seguro, por lo cual, personas dentro y fuera de la Organización pueden encontrar formas de tener acceso a la información. De acuerdo con lo anterior, la Organización no puede garantizar la

	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

confidencialidad absoluta de la información almacenada en cualquier dispositivo perteneciente a la empresa y por ende la privacidad de los usuarios.

- ✓ Información clasificada. Es deber de todo el personal cuidar y proteger la información de carácter confidencial o clasificada como sensible, usando las herramientas que la empresa le proporciona para tal fin.
- ✓ El uso de medios removibles (dispositivo de almacenamiento externos) y/o Unidades ópticas, para la extracción de información será restringido y solo personal autorizado podrá utilizarlas.
- ✓ Acceso restringido a centro de cableados y datos. Está prohibido el ingreso a centros de cableados o de datos sin el visto bueno de la unidad de informática.
- ✓ Reparación y mantenimiento de equipos. El personal de soporte técnico de Informática tiene la autoridad para acceder a archivos individuales o datos cada vez que deban realizar mantenimientos, reparación o chequeo de equipos de computación. Sin embargo, el personal de soporte técnico a cargo de Informática debe garantizar la confidencialidad y custodia en el manejo de la información a la cual tiene acceso y no puede exceder su autoridad en ninguna de estas eventualidades para usar esta información con propósitos diferentes al de mantenimiento y reparación.
- ✓ Respuesta al uso indebido de computadores y sistemas de información. Cuando por alguna causa razonable denominada así por el responsable de la unidad de informática o por quién haga sus veces, se sospeche de algún tipo de uso indebido como se describe en la sección nueve (5.7) de este documento, la Unidad de Informática puede acceder cualquier cuenta, datos, archivos o servicio de información perteneciente a los involucrados en el incidente, para investigar y de acuerdo con los hallazgos o evidencias, dar traslado a la unidad respectiva y/o a la unidad de Talento Humano para que éstos, de acuerdo con el marco de actuación, reglamentos, normas y políticas de la Organización apliquen las acciones respectivas.
- ✓ Monitoreo de la Red empresarial y los Servicios. Debido a que la Organización se esforzará en mantener la privacidad de las comunicaciones personales y un nivel de servicio apropiado, la Unidad de Informática monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes. Además, se recolectarán estadísticas de utilización basado en las

	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	


direcciones de red, protocolo de red y tipo de aplicación. Progresivamente se restringirán usuarios y aplicaciones no esenciales cuando su utilización en la red resulte en la degradación del rendimiento. Tal restricción será notificada a los usuarios a través de los medios apropiados.

### **5.9. Instalación y Uso de Software**

- ✓ De acuerdo con las normas locales e Internacionales relativas a los derechos de propiedad intelectual, el único software que será instalado en el computador del usuario será aquel que previamente haya sido estandarizado y/o autorizado por la Organización y para lo cual ésta dispone de las licencias respectivas a su nombre.
- ✓ El usuario no deberá participar en la copia, distribución, transmisión o cualquier otra práctica no autorizada en las licencias de uso de software.
- ✓ El usuario no tiene permitido la instalación de software de “dominio público” o de “distribución libre” (Shareware y Freeware).
- ✓ Toda instalación, desinstalación o traslado de software (incluyendo aquellos de “dominio público” de “distribución libre”) desde y hacia un equipo Organizacional debe efectuarse directamente por la Unidad de Informática.
- ✓ Cualquier software que se haya instalado en un equipo Organizacional que no cumpla con lo estipulado anteriormente, será desinstalado sin que ello derive ninguna responsabilidad para la Organización.
- ✓ Al usar una licencia de software que ha sido instalado en un equipo Institucional o en un equipo Personal, el usuario reconoce los derechos de la Organización anteriormente descritos y es consiente en ellos.
- ✓ El uso de programas ejecutables no instalables, conocidos como portables, no deben usarse sin el visto bueno de la Unidad de Informática.
- ✓ Está prohibido el uso de software de tipo Anonimato o cualquier otro similar que permita evadir las restricciones de navegación definidas por la organización.

### **5.10. Correo electrónico y demás herramientas colaborativas disponibles**

- ✓ Todas las políticas incluidas en este documento son aplicables al Correo Electrónico.

	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

- ✓ El correo electrónico debe usarse de manera profesional y cuidadosa dada su facilidad de envío y redirección. Los usuarios deben ser especialmente cuidadosos con los grupos de destinatarios, chats y foros de discusión. Las leyes de derechos de autor y licencias de software también aplican para correo electrónico.
- ✓ Los mensajes de correo electrónico de la Organización en el dominio de esta deben ser utilizados para uso estrictamente laboral.
- ✓ Para hacer una óptima utilización de la capacidad del buzón de mensajes, los mensajes de correo electrónico en los dominios pertenecientes a la Organización deben ser borrados una vez que la información contenida en ellos ya no sea de utilidad.
- ✓ En ningún caso es permitido suplantar las cuentas de usuarios ajenos.


#### **5.11. Páginas Web y Sistema de contenido en Redes Sociales**

El responsable de custodiar la Marca e Imagen de la empresa y el Gerente General de la Unidad de Negocio, acogiendo la directriz organizacional, determinará los estándares para aquellos contenidos considerados como oficiales de la Organización y publicados en su página web; ninguna otra página o contenido electrónico puede hacer uso de los logos de la Organización sin la autorización expresa del director de la Unidad de Mercadeo o quién haga sus veces.

Los editores de las páginas Web o usuarios que hagan sus veces, que usen información asociada con la Organización deben acogerse a las políticas de la Organización misma, a la ley que las regula incluyendo derechos de autor, leyes sobre obscenidad, calumnia, difamación y piratería de software. El contenido debe ser revisado periódicamente y autorizado por el responsable de custodiar la Marca e Imagen de la empresa y/o Gerente General de la Unidad de Negocio.

#### **5.12. Incumplimiento de las políticas de uso responsable de los sistemas de información y recursos informáticos de la organización**

- ✓ La Organización hará responsable al usuario de las Políticas y las consecuencias que se derivarían de su incumplimiento. Así mismo, el usuario deberá conocer estas políticas desde su ingreso a la Organización.

	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

- ✓ La Organización se reserva el derecho de evaluar periódicamente el cumplimiento de estas Políticas. Cualquier acción disciplinaria derivada del incumplimiento de esta, tales como llamadas de atención, suspensiones o despidos, serán consideradas, de acuerdo con los procedimientos establecidos por la Organización y estricto acato de las políticas internas de la compañía respetando las estipulaciones legales vigentes.
- ✓ En materia de irregularidades o incumplimiento en el uso del software, el usuario que no cumpla con estas políticas será directamente responsable de las acciones disciplinarias o sanciones por entes externos, que, por la responsabilidad laboral, penal y/o civil se incurra, derivadas de sus propios actos. Igualmente será responsable de los costos y gastos en que pudiera incurrir la Organización derivados de la defensa por el uso no autorizado o indebido de licencias de software. Debido a lo anterior, no es permitido alegar ignorancia ni a estas políticas, ni a la documentación que en las licencias de software se mencione, incluyendo por supuesto las demás licencias en uso.
- ✓ En el caso en que razonablemente se asuma que se está haciendo uso ilegal o incorrecto de los servicios informáticos o sistemas de información, la Organización estará en absoluta libertad de limitar o remover las cuentas asignadas sin asumir por ello ninguna responsabilidad de ningún tipo.

## 6. RESPONSABLES


### 6.1. Es responsabilidad de **Talento Humano:**

- ✓ Gestionar cualquier sanción o acción disciplinaria a los colaboradores que no cumplan con lo estipulado en la política según la base legal mencionada en el documento.
- ✓ Divulgar la política a todos los colaboradores, proveedores, contratistas, consultores, aprendices y a cualquier otra persona que tenga acceso a los sistemas de información de Aceros Abonos Agro.

### 6.2. Es responsabilidad del **Supervisor de área o Jefatura Inmediata:**

- ✓ Velar por cumplimiento de la política en su Departamento.
- ✓ En los casos que sea necesario, realizar las solicitudes pertinentes para que sus colaboradores cuenten con el equipo de Tecnología de Información adecuado para la ejecución de sus funciones.




	<b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

**6.3. Es responsabilidad del **Tecnologías de Información:****

- ✓ Tramitar la entrega del Equipo Tecnológico a los colaboradores que lo requieran para cumplir con sus funciones laborales.
- ✓ Determinar, en caso de daño al equipo tecnológico si es una falla técnica o por negligencia del colaborador.
- ✓ Diligenciar toda actividad estipulada en la política que incluya la participación del Departamento.


**6.4. Es responsabilidad del **Colaborador:****


- ✓ Cuidar y mantener en buen estado el equipo suministrado por la compañía.
- ✓ Cumplir con las disposiciones de esta política con el uso de las tecnologías de información.
- ✓ Firmar el documento “Contrato de condiciones de entrega y uso de herramientas de Tecnologías de Información propiedad de Aceros Abonos Agro S.A”


 <b>ABONOS AGRO</b>	<b>Política Uso de Tecnologías de Información</b>	Código	AAA-POL-015
		Revisión	1
		Fecha	
		Realizado por	Gestión de Procesos
		Aprobado por	


## 7. ANEXOS


### 7.1. Anexo N°1. Contrato de condiciones de entrega y uso de herramientas de Tecnologías de Información propiedad de Aceros Abonos Agro


 <b>ABONOS AGRO</b>	<b>CONTRATO DE CONDICIONES DE ENTREGA Y USO DE HERRAMIENTAS DE TECNOLOGÍAS DE INFORMACIÓN PROPIEDAD DE ACEROS ABONOS AGRO S.A.</b>
Fecha: _____	
<p>YO</p> <p><i>CEDULA DE IDENTIDAD #</i></p> <p><i>FUNCIONARIO DE <u>Aceros Abonos Agro</u></i></p> <p><i>DEPARTAMENTO DE</i></p>	
<p><i>HAGO CONSTAR QUE HE RECIBIDO DEL DEPARTAMENTO DE TECNOLOGIA DE INFORMACION, UN EQUIPO CON LAS SIGUIENTES CARACTERÍSTICAS:</i></p>	
<p><i>TIPO DE EQUIPO:</i></p> <p><i>MARCA:</i></p> <p><i>MODELO:</i></p> <p><i>NUMERO DE SERIE:</i></p> <p><i>PLACA ACTIVO:</i></p> <p><i>SE HA INSTALADO ONE DRIVE PARA RESPALDOS Si <input type="checkbox"/> No <input type="checkbox"/></i></p> <p><i>Adaptador HDMI a VGA Si <input type="checkbox"/> No <input type="checkbox"/></i></p>	
<p><i>PARA SER UTILIZADO EN MIS FUNCIONES PROPIAS, ACEPTANDO LAS DISPOSICIONES QUE A CONTINUACION SE DETALLAN:</i></p>	
<p><b>1. Sobre el uso del Activo:</b></p> <p>a. El equipo entregado será usado como una herramienta de trabajo para uso exclusivo de las actividades laborales asignadas a la persona, en ninguna circunstancia el equipo podrá ser utilizado para fines personales o fines lucrativos</p>	
Page 1 of 4	


 <b>Política Uso de Tecnologías de Información</b>	<b>Código</b>	<b>AAA-POL-015</b>
	<b>Revisión</b>	<b>1</b>
	<b>Fecha</b>	
	<b>Realizado por</b>	<b>Gestión de Procesos</b>
	<b>Aprobado por</b>	


 ACEROS ABONOS AGRO	<b>CONTRATO DE CONDICIONES DE ENTREGA Y USO DE HERRAMIENTAS DE TECNOLOGÍAS DE INFORMACIÓN PROPIEDAD DE ACEROS ABONOS AGRO S.A.</b>
<p>b. Todas las licencias de Software instaladas en el equipo son propiedad de ACEROS ABONOS AGRO S.A., por lo tanto, no se permitirá la instalación de software de cualquier tipo sin la autorización del departamento de tecnología.</p> <p>c. El equipo deberá ser devuelto al departamento de tecnología en el mismo estado de funcionamiento que tenía cuando se le entregó, salvo el deterioro normal por el uso del activo en el transcurrir del tiempo.</p> <p>d. Si durante el periodo de uso del equipo se diera una modificación en las funciones del puesto, que afecte la justificación original del equipo entregado, el empleado debe notificar tal situación al departamento de tecnología.</p>	
<p><b>2. Sobre el cuidado del Activo:</b></p> <p>a. El empleado será responsable por cualquier daño que sufra el equipo por mala manipulación, descuido y/o irresponsabilidad, ajeno al deterioro normal por el uso en su trabajo.</p> <p>b. Por causas atribuibles al empleado, en caso de pérdida total del equipo, o daño que no permita su reparación para reintegrarlo a su uso regular, el empleado acepta asumir todos los gastos en que la empresa incurra, tanto para reponer el equipo por uno de características similares, como aquellos que se requieran para reintegrarlo a su anterior condición de uso.</p> <p>c. En caso de que el equipo presente fallas, es responsabilidad del empleado reportarlo de INMEDIATO al Departamento de TI para su reparación o sustitución; en caso de que se compruebe negligencia por parte del empleado en reportes tardíos se aplica la cláusula 2.b.</p>	
<p><b>3. Sobre los Seguros y/o Pérdida del Activo:</b></p> <p>a. El empleado se compromete en caso de robo a reportarlo inmediatamente al Organismo de Investigación Judicial, levantar una denuncia y solicitar la inspección ocular respectiva. Estos documentos deben ser entregados a la mayor brevedad al departamento de T.I para el debido trámite.</p> <p>b. Si NO existe una denuncia formal ante un organismo policial acreditado que pueda servir para los trámites ante la aseguradora, el empleado deberá</p>	
<p>Page 2 of 4</p>	

 <b>ACEROS</b> ABONOS AGRO	<h2>Política Uso de Tecnologías de Información</h2>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	


 <b>ACEROS</b> ABONOS AGRO	<h3>CONTRATO DE CONDICIONES DE ENTREGA Y USO DE HERRAMIENTAS DE TECNOLOGÍAS DE INFORMACIÓN PROPIEDAD DE ACEROS ABONOS AGRO S.A.</h3>
<p>asumir el pago del activo de acuerdo con el valor en libros al momento del robo.</p>	
<p>c. Si la compañía aseguradora refuta el pago correspondiente por el seguro del activo con causas justificadas atribuibles al empleado este deberá asumir todos los gastos en que la empresa incurra, tanto para reponer el equipo por uno de características similares, como aquellos que se requieran para reintegrarlo a su condición de uso normal.</p>	
<p><b>4. Sobre la información y su respaldo:</b></p>	
<p>a. TI instalará la aplicación OneDrive en cada equipo para el respectivo respaldo de la información.          Todo usuario es responsable de mantener respaldos de la información de acuerdo con sus necesidades, en la nube de la empresa OneDrive.</p>	
<p>b. Es prohibido a todos los funcionarios de cualquier nivel, utilizar el equipo de la oficina para bajar de internet: juegos, música, videos, fotos, protectores de pantalla y todo archivo que provenga de fuentes no confiables; así como todo tipo de material pornográfico, que atenta contra el trabajo o el honor de las personas.</p>	
<p>c. Será responsabilidad del empleado el mantener la debida seguridad de sus archivos de datos en el equipo cumpliendo las siguientes normas:</p>	
<p style="padding-left: 40px;"><i>i. Utilización de una llave de acceso en el BIOS (Password de encendido) el cual será asignado y controlado por Infraestructura.</i></p>	
<p style="padding-left: 40px;"><i>ii. Uso de protector de pantalla con password para evitar la manipulación incorrecta del equipo sin la autorización de su dueño.</i></p>	
<p style="padding-left: 40px;"><i>iii. Uso de llaves de acceso (password) para los archivos de datos importantes.</i></p>	
<p>d. El equipo deberá ser devuelto al departamento de tecnología o a la jefatura correspondiente de inmediato en caso de finalización de la relación laboral por cualquier motivo, se le dará un respaldo solo de sus archivos personales una vez comprobado su contenido y aprobado por el superior.</p>	
<p>Page 3 of 4</p>	

	<b>Política Uso de Tecnologías de Información</b>	Código	AAA-POL-015
		Revisión	1
		Fecha	
		Realizado por	Gestión de Procesos
		Aprobado por	

	<b>CONTRATO DE CONDICIONES DE ENTREGA Y USO DE HERRAMIENTAS DE TECNOLOGÍAS DE INFORMACIÓN PROPIEDAD DE ACEROS ABONOS AGRO S.A.</b>
<p>e. Para que un equipo sea recibido y aceptado de conformidad por el departamento de tecnología, el mismo debe estar en las mismas condiciones en que fue entregado, salvo el desgaste físico debido al correcto uso de este y al transcurrir del tiempo.</p>	
<p><b>5. Sobre situaciones irregulares de daños, hurto/robo, desperfectos/desmejoras y otros</b></p>	
<p>La Empresa procederá a realizar la investigación, y si esta determina la responsabilidad del trabajador sobre estos y por acciones que se determinen como dolo (intención) o culpa (negligencia, imprudencia o impericia), se expondrá a sanciones disciplinarias y el despido.]</p>	
<p><i>Estas condiciones están sujetas a revisión y cambios por parte de la compañía, los cuales serán comunicados oportunamente.</i></p>	
<p><b>NOTA:</b></p>	
<p><b>UNA VEZ LEIDO, DECLARO QUE CONOZCO Y ACEPTO LAS DISPOSICIONES BAJO LAS CUALES SE REGULARÁ LA RESPONSABILIDAD A LA QUE QUEDO SUJETO AL RECIBIR Y HACER USO DEL EQUIPO DE COMPUTO DE ACEROS ABONOS AGRO S.A.</b></p>	
<p>FIRMO EN CONFORMIDAD EN LA FECHA: _____.</p>	
<p><u>Nombre y Firma del usuario del equipo que recibe</u></p> <p>_____</p>	
<p><u>Nombre y Firma del funcionario del Departamento de Tecnología que entrega</u></p> <p>_____</p>	
<p>CC/ para el interesado.</p>	
<p>Page 4 of 4</p>	

	<h2>Política Uso de Tecnologías de Información</h2>	<b>Código</b>	<b>AAA-POL-015</b>
		<b>Revisión</b>	<b>1</b>
		<b>Fecha</b>	
		<b>Realizado por</b>	<b>Gestión de Procesos</b>
		<b>Aprobado por</b>	

### 7.2 Anexo N°2. Proceso de Investigación



### Proceso de Investigación

*Sobre situaciones irregulares de daños, hurto/robo, desperfectos/desmejoras y otros*

La Empresa procederá a empezar una investigación, y si esta determina la responsabilidad del trabajador sobre estos y por acciones que se determinen como dolo (intención) o culpa (negligencia, imprudencia o impericia) entonces se le generará al trabajador las siguientes opciones:

Esta investigación siempre se debe realizar y documentarse de la siguiente forma:

Reporte de incidente disciplinario que detalle:

- ¿Qué pasó?
- ¿Cuándo pasó?
- ¿Dónde pasó?
- Consecuencias del incidente
- Pruebas tomadas: videos, fotos, testigos.
- En caso de robo/hurto la correspondiente copia de la denuncia correspondiente
- Reporte detallado de los daños y del costo de reparación o reposición con las respectivas cotizaciones
- Manifestaciones de testigos.

Con todo lo anterior, se le hace una entrevista al empleado, para que éste tenga conocimiento de la investigación y de las pruebas e indique de manera expresa:

a. Si acepto la responsabilidad y estoy de acuerdo en la deducción.  
b. NO acepto la responsabilidad y no estoy de acuerdo en ningún rebajo y procedan como a bien lo tengan.

En el primer caso, se aplica los formularios de:

a. Vale de anticipo de salario.  
b. Solicitud de anticipo de salario.  
c. Autorización por deducción por planilla de anticipo de salario.  
d. Sanción disciplinaria ponderando que el trabajador aceptó la situación y el rebajo

La deducción se aplicará considerando los artículos 36, 172 y 173 Código de Trabajo, en lo que interesa:

a. Aplicando la fórmula de embargo de salario.  
b. En no menos de 4 tramos a partir del próximo periodo de pago.

En el segundo caso, se aplica la sanción disciplinaria más grave, lo cual se debe hacer dentro del mes siguiente a que los hechos fueron conocidos o el patrono adquirió conocimiento de estos y la sanción se debe aplicar considerando los incisos a) y b) del art. 71 en su relación con el art. 81 inciso d) y l) del Código de Trabajo.

- ✓ Aceptar la responsabilidad y firmar los formatos de solicitud de anticipo y deducción de salario para cubrir el valor total del daño y la Empresa por cada dinero retenido le dará un vale por anticipo de salario y paralelamente se impone sanción que puede ser desde amonestación verbal hasta suspensión sin goce de salario sustitutiva de un despido sin responsabilidad patronal, de acuerdo con la gravedad del hecho.
- ✓ Negar la responsabilidad, y la Empresa decide aplicar el despido sin responsabilidad patronal con fundamento en los incisos d) y l) del art. 81 del Código de Trabajo por falta grave derivada de los daños incurridos, pero para esto se requiere, que se cuente con una investigación completa y documentada y que además la Empresa no tenga otro tipo de contingencias (horas extra, CCSS, salarios mínimos, etc.).
- ✓ Si la investigación no determina su responsabilidad, la empresa debe cerrar el caso.]

### 8. CONTROL DE CAMBIOS

Versión	Fecha de vigencia	Modificación	Responsable
1		Inclusión de portada, control de cambios, 1° versión de política.	Gestión de procesos